

10/507212

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2001-126009

(P2001-126009A)

(43)公開日 平成13年5月11日 (2001.5.11)

| | | | |
|--------------|-------|--------------|-------------------|
| (51) Int.Cl' | 識別記号 | F I | テ-マコ-ト(参考) |
| G 06 F 19/00 | | G 09 C 1/00 | 6 6 0 C 5 B 0 4 9 |
| 17/60 | | G 06 F 15/30 | L 5 B 0 5 5 |
| 17/30 | | 15/21 | 3 4 0 A 5 B 0 7 5 |
| G 09 C 1/00 | 6 6 0 | 15/30 | M 5 J 1 0 4 |

3 4 0

審査請求 未請求 請求項の数13 OL (全 14 頁) 最終頁に続く

(21)出願番号 特願平11-310090

(22)出願日 平成11年10月29日 (1999.10.29)

(71)出願人 000004226
 日本電信電話株式会社
 東京都千代田区大手町二丁目3番1号

(72)発明者 藤村 考
 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

(72)発明者 松山 一雄
 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

(74)代理人 100070150
 弁理士 伊東 忠彦

最終頁に続く

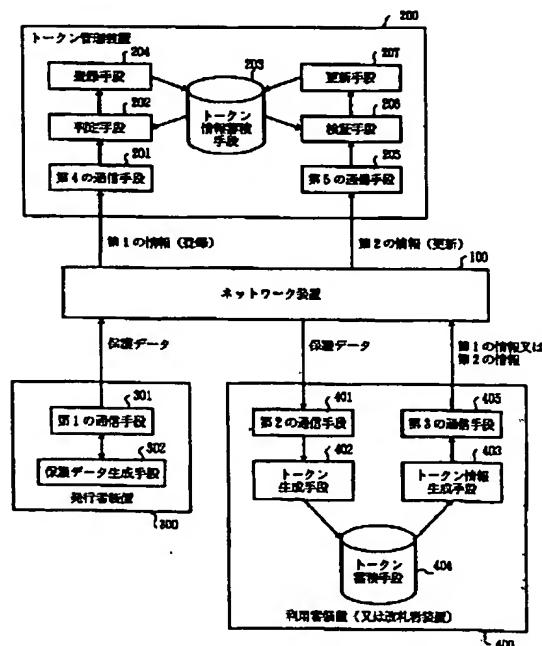
(54)【発明の名称】電子情報流通システム及び電子情報流通プログラムを格納した記憶媒体及び電子情報流通方法

(57)【要約】 (修正有)

【課題】保護データの所有者を効率的に認証でき、誰でも利用できる汎用的な電子情報流通方法及びシステムを提供する。

【解決手段】多重使用を防止すべき保護データを生成し、送信する発行者装置と、保護データを受信し、保護データの所有者を特定する情報であるトークンと、トークンを特定するトークン情報を生成して、蓄積し、保護データを特定する保護データIDとトークン情報を含む第1の情報を送信する利用者装置と、第1の情報を受信し、保護データIDと等しい値を持つ第1の情報が既に蓄積されているかを判定し、蓄積されていない時の第1の情報を蓄積し、既に蓄積されている第1の情報を特定する保護データIDと更新後のトークン情報を含む第2の情報を受信し、第2の情報の送信元の装置が第1の情報に含まれるトークン情報をによって特定される保護データを保有している時のみ第1の情報を更新するトークン管理装置とを有する。

本発明の原理構成図



【特許請求の範囲】

【請求項 1】 電子的な情報の流通を行う情報流通システムであって、電子情報であり、多重使用を防止すべき保護データを生成する保護データ生成手段と、前記保護データを送信する第1の通信手段とを有する発行者装置と、前記保護データを受信する第2の通信手段と、前記保護データの所有者を特定する情報であるトークンを生成するトークン生成手段と、前記トークンを特定するトークン情報を生成するトークン情報生成手段と、前記トークンを蓄積するトークン蓄積手段と、前記保護データを特定する保護データIDと前記トークン情報を含む第1の情報を送信する第3の通信手段とを有する利用者装置と、前記第1の情報を受信する第4の通信手段と、前記保護データIDと等しい値を持つ前記第1の情報が既に蓄積されているかを判定する判定手段と、前記判定手段において蓄積されていない時のみ前記第1の情報を蓄積する蓄積手段と、既に蓄積されている前記第1の情報に対する更新情報をとして該第1の情報を特定する前記保護データIDと更新後のトークン情報を含む第2の情報を受信する第5の通信手段と、前記第2の情報の送信元の装置が前記第1の情報に含まれるトークン情報によって特定される前記保護データを保有していることを検証する検証手段と、前記検証手段において保有している時のみ前記第1の情報を更新する更新手段とを有するトークン管理装置と、前記発行者装置、前記利用者装置、前記トークン管理装置とを接続するネットワーク装置とを有することを特徴とする電子情報流通システム。

【請求項 2】 前記利用者装置の前記トークン情報生成手段は、前記トークンに対する一方向性関数の出力を利用して、前記トークン情報を生成する手段を含み、前記トークン管理装置の前記検証手段は、前記第2の情報の送信元から前記トークンを受信し、該トークンに対する一方向性関数の出力値が、更新対象の前記第1の情報に記録されているトークン情報に一致するかを検証する手段を含む請求項1記載の電子情報流通システム。

【請求項 3】 前記トークン管理装置は、前記蓄積手段に蓄積されている前記第1の情報に対する更新を行うために受信する前記第2の情報には、さらに、該第1の情報に含まれるトークン情報によって特定されるトークンを含み、該第2の情報の送信元の装置が、前記トークンを保有していることを判別する手段を含む請求項1または、2記載の電子情報流通システム。

【請求項 4】 前記トークン管理装置は、前記保護データIDを受信する手段と、前記トークン情報蓄積手段に蓄積されている前記第1の情報の中から前記保護データIDが含まれる第1の情報を検索し、該第1の情報に含まれる前記トークン情報を送信する手段とを更に有し、前記利用者装置は、前記トークン情報を受信する手段と、蓄積されている前記保護データIDによって特定される前記保護データの所有者を特定するトークンに対する一方向性関数の出力値が、前記トークン情報と一致しているかどうかを検証する手段を更に有する請求項2または、3記載の電子情報流通システム。

【請求項 5】 前記トークン管理装置は、前記第1の情報及び前記第2の情報に含まれる保護データIDに、前記保護データに対する一方向性関数の出力を含む請求項1、2、3、または、4記載の電子情報流通システム。

【請求項 6】 前記保護データIDに、前記保護データのネットワーク上のアドレスを含む請求項1、2、3、4または、5記載の電子情報流通システム。

【請求項 7】 電子的な情報の流通を行う電子情報流通システムにおいて、トークンを特定するトークン情報を管理するトークン管理装置に搭載される電子情報流通プログラムを格納した記憶媒体であって、利用者装置で生成された保護データを特定する保護データIDとトークン情報を含む第1の情報を受信させる第1の通信プロセスと、前記保護データIDと等しい値を持つ前記第1の情報が既に蓄積されているかを判定する判定プロセスと、前記判定プロセスにおいて蓄積されていない時のみ前記第1の情報を蓄積手段に格納する格納プロセスと、既に前記蓄積手段に格納されている前記第1の情報に対する更新情報をとして該第1の情報を特定する前記保護データIDと更新後の新しいトークン情報を含む第2の情報を受信する第2の通信プロセスと、前記第2の情報の送信元の装置が前記第1の情報に含まれるトークン情報によって特定される前記トークンを保有していることを検証する検証プロセスと、前記検証プロセスにおいて保有している時のみ前記第1の情報を更新する更新プロセスとを有することを特徴とする電子情報流通プログラムを格納した記憶媒体。

【請求項 8】 前記検証プロセスは、前記第2の情報の送信元から前記トークンを受信し、該トークンに対する一方向性関数の出力値が、更新対象の前記第1の情報に記録されているトークン情報に一致するかを検証するプロセスを含む請求項7記載の電子情報流通プログラムを格納した記憶媒体。

【請求項 9】 前記前記蓄積手段に蓄積されている前記第1の情報に対する更新を行うために受信する前記第2

の情報には、さらに、該第1の情報に含まれるトークン情報によって特定されるトークンを含み、該第2の情報の送信元の装置が、前記トークンを保有していることを判別するプロセスを含む請求項7または、8記載の電子情報流通プログラムを格納した記憶媒体。

【請求項10】前記保護データIDを受信する第3の通信プロセスと、

前記蓄積手段に格納されている前記第1の情報の中から前記保護データIDが含まれる第1の情報を検索し、該第1の情報に含まれる前記トークン情報を送信するプロセスと更に有する請求項8または、9記載の電子情報流通プログラムを格納した記憶媒体。

【請求項11】電子的な情報の流通を行うための電子情報流通方法において、

多重使用を防止すべき保護データを発行する際に、発行者装置において、保護データを生成し、利用者装置に転送し、

前記利用者装置が前記保護データを受け取ると、該保護データ毎にトークンを生成して格納しておき、該トークンと該保護データからハッシュ値で表現される保護データIDとトークン情報を含む発行要求を生成して、該発行者装置に転送し、

前記発行者装置は、前記発行要求に含まれている前記トークン情報と前記保護データIDを含むトークン情報登録要求を生成し、トークン管理装置に転送し、

前記トークン管理装置は、前記トークン情報登録要求に含まれている前記保護データIDが蓄積されているかを判定し、蓄積されていない場合に、該保護データIDに対応するトークン情報を登録することを特徴とする電子情報流通方法。

【請求項12】前記保護データを譲渡する際に、譲渡元の前記利用者装置において、譲渡対象の保護データを指定し、譲渡先の利用者装置に該保護データを転送し、

譲渡先の利用者装置は、前記保護データに対応する新たなトークンを生成して格納しておき、

前記保護データと前記新たなトークンのハッシュ値で表現されるトークン情報を含む譲渡要求を生成して、前記譲渡元の利用者装置に該譲渡要求を転送し、

前記譲渡元の利用者装置は、蓄積されている譲渡対象の保護データに対するトークンを取得し、前記譲渡要求に含まれている該保護データに対する新しいトークン情報と保護データIDと前記トークンとを含むトークン情報更新要求を生成し、トークン管理装置に該トークン情報更新要求を転送し、

前記トークン管理装置は、前記トークン情報更新要求に含まれている前記トークンのハッシュ値と、予め蓄積されているトークン情報と一致するかを判定し、等しい場合に、前記保護データのトークン情報を更新する請求項11記載の電子情報流通方法。

【請求項13】前記保護データを消費する際に、前記利用者装置は、保護データ要求条件を受け取ると、その条件に合致する保護データを予め保護データが格納されている記憶手段から検索し、検索された保護データに対するトークンを取得し、改札者装置に該トークンと該保護データとを転送し、前記改札者装置は、前記保護データのハッシュ値で表現される保護データIDと前記トークンを含むトークン情報削除要求を生成し、前記トークン管理装置に該削除要求を転送し、

前記トークン管理装置は、前記トークン情報削除要求に含まれている前記トークンのハッシュ値と予め蓄積されているトークン情報と一致するかを判定し、等しい場合に、前記保護データのトークン情報を無効にする請求項11記載の電子情報流通方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、電子情報流通システム及び電子情報流通プログラムを格納した記憶媒体及び電子情報流通方法に係り、特に、チケットやクーポン等のサービスや物を請求する権利をデジタル化した電子チケット、あるいはお金や商品券等の価値をデジタル化した電子現金のように、利用者間で転々と流通し、かつ不正な複製を防止することが必要な電子情報について、正当な電子情報の所有者を認証することを可能とする汎用的な電子情報流通システム及び電子情報流通プログラムを格納した記憶媒体及び電子情報流通方法に関するもの。

【0002】

【従来の技術】電子チケットや電子現金などは、一般に、複製が作られることを防止、もしくは、複製された場合に、本物と識別することが求められる。即ち、配布したデータが利用者等により複製され、それらが多重に使用されることを防ぐ必要がある。

【0003】従来は、以下で示すような技術により、上記のような多重使用を防止しなければならないデータ（以後、保護データと呼ぶ）を流通させている。第1の方法は、保護データをICカード等の耐タンパ装置に格納し、当該データを耐タンパ装置の外からは参照できないようにする。そして、当該データを利用者から利用者へ譲渡する場合には、当該耐タンパ装置間で暗号化して移動させる。譲渡者の耐タンパ装置から被譲渡者への耐タンパ装置への移動が成功した場合には、確実に譲渡者の耐タンパ装置から当該データを抹消する。これにより、各保護データが複製されないように制御する。また、保護データを使用する場合には、当該保護データを該耐タンパより抹消する。これらにより、保護データが多重譲渡あるいは多重使用されることを防止する。

【0004】このような方式の例としては、例えば、特願平6-503913や、特表平9-511350等多

数存在し、さらに、特願平11-39080や、特願平11-247457では、保護データ自身は通常の蓄積媒体に格納するが、当該データの原本性を示すデータ（トークン）のみを耐タンパ装置に格納することで、処理速度や記憶容量等に関して効率を向上させる方法等多数の方法が提案されている。

【0005】第2の方法は、保護データとそのデータの所有者の識別子をセンタDBによって管理するものである。この方法は、保護データを利用者から利用者へ譲渡する場合に、譲渡者は、当該データに対する譲渡証明書をセンタに送り、当該データの所有者の変更を依頼する。そして、これを受け取ったセンタは、DBに管理している当該データの所有者を譲渡証明書に記述された譲受者の識別子に書き換えるという方法により、各保護データに対する所有者が必ず一人になるように制御する。また、保護データを使用する場合には、使用者は、保護データに対する使用証明書をセンタに送り、当該データを使用済状態への変更を依頼する。そして、これを受け取ったセンタは、DBに管理している当該データを使用済状態に変更する。これらにより、保護データが多重譲渡あるいは、多重使用することを防止する。このような方式としては、例えば、Peter Wayner, Digital Cash, 2nd Edition, Academic Press Ltd. 等に多数の方法が紹介されている。

【0006】

【発明が解決しようとする課題】しかしながら、上記従来の第1の方法は、システムのセキュリティが耐タンパ装置に依存し、耐タンパ装置が破られた場合の被害が大きいという問題がある。また、性能面でもシステム全体の性能が耐タンパ装置の性能に依存し、特に、耐タンパとしてICカードを利用した場合には、ICカードがボトルネックとなる場合が多い。さらに、ICカードを使用するにあたっては、ICカードリーダーのような物理的な装置が必要であるが、これが利用者端末に普及していないという問題がある。

【0007】上記従来の第2の方法は、センタで管理するため、保護データを譲渡あるいは、行使する際には、ネットワークに接続しなければならないという問題がある。この点を除いては、第1の方法に比較して、実現が比較的容易である等のメリットがある。また、ネットワークのコストが近年著しく低下してきている等の理由から、ネットワークの接続は大きなデメリットとはならなくなってきた。

【0008】但し、第2の方法を実現する手段として、従来、譲渡証明書や使用証明書を譲渡者あるいは使用者のデジタル署名が用いられてきたが、デジタル署名では、一般に公開鍵証明書で定義された利用者識別子によって、署名者を識別する方法がとられているが、この方法では、事前に公開鍵証明書の取得や交換を行うことが必要であり、これにより、処理効率の低下や、利用者

識別子が明らかになることによるプライバシ上の問題等がある。

【0009】また、第2の方法におけるセンタDBの運営は、従来、保護データの生成者であるサービス提供者自身が行うのが一般的であるが、この方法では、サービス提供者毎にセンタDBを運営するためコストがかかる。また、サービス提供者が勝手にセンタDB上にある保護データを削除あるいは改ざんしても、利用者は手元に保護データを持たないので、その証拠を提示するのが困難である等の問題がある。

【0010】本発明は、上記の点に鑑みなされたもので、従来の第2の方法において、公開鍵証明書の取得や、交換を必要とする公開鍵を使用せずに、ハッシュ関数のみで保護データの所有者を効率的に認証でき、かつ、内容によらず誰でも利用できる汎用的な電子情報流通システム及び電子情報流通プログラムを格納した記憶媒体及び電子情報流通方法を提供することを目的とする。

【0011】

【課題を解決するための手段】図1は、本発明の原理構成図である。本発明（請求項1）は、電子的な情報の流通を行う情報流通システムであって、電子情報であり、多重使用を防止すべき保護データを生成する保護データ生成手段302と、保護データを送信する第1の通信手段301とを有する発行者装置300と、保護データを受信する第2の通信手段401と、保護データの所有者を特定する情報であるトークンを生成するトークン生成手段402と、トークンを特定するトークン情報を生成するトークン情報生成手段403と、トークンを蓄積するトークン蓄積手段404と、保護データを特定する保護データIDとトークン情報を含む第1の情報を送信する第3の通信手段405とを有する利用者装置400と、第1の情報を受信する第4の通信手段201と、保護データIDと等しい値を持つ第1の情報が既に蓄積されているかを判定する判定手段202と、判定手段202において蓄積されていないのみ第1の情報を蓄積するトークン情報蓄積手段203と、トークン情報蓄積手段203に第1の情報を登録する登録手段204と、既に蓄積されている第1の情報に対する更新情報をとして該第1の情報を特定する保護データIDと更新後のトークン情報を含む第2の情報を受信する第5の通信手段205と、第2の情報の送信元の装置が第1の情報に含まれるトークン情報によって特定される保護データを保有していることを検証する検証手段206と、検証手段206において保有している時のみ第1の情報を更新する更新手段207とを有するトークン管理装置200と、発行者装置300、利用者装置400、トークン管理装置200とを接続するネットワーク装置100とを有する。

【0012】本発明（請求項2）は、利用者装置400

のトークン情報生成手段403において、トークンに対する一方向性関数の出力をを利用して、トークン情報を生成する手段を含み、トークン管理装置200の検証手段206において、第2の情報の送信元からトークンを受信し、該トークンに対する一方向性関数の出力値が、更新対象の第1の情報に記録されているトークン情報に一致するかを検証する手段を含む。

【0013】本発明（請求項3）は、トークン管理装置200において、トークン情報蓄積手段203に蓄積されている第1の情報に対する更新を行うために受信する第2の情報には、さらに、該第1の情報に含まれるトークン情報によって特定されるトークンを含み、該第2の情報の送信元の装置が、トークンを保有していることを判別する手段を含む。

【0014】本発明（請求項4）は、トークン管理装置200において、保護データIDを受信する手段と、トークン情報蓄積手段203に蓄積されている第1の情報の中から保護データIDが含まれる第1の情報を検索し、該第1の情報に含まれるトークン情報を送信する手段とを更に有し、利用者装置400において、トークン情報を受信する手段と、蓄積されている保護データIDによって特定される保護データの所有者を特定するトークンに対する一方向性関数の出力値が、トークン情報と一致しているかどうかを検証する手段を更に有する。

【0015】本発明（請求項5）は、トークン管理装置200において、第1の情報及び第2の情報に含まれる保護データIDに、保護データに対する一方向性関数の出力を含む。本発明（請求項6）は、保護データIDに、保護データのネットワーク上のアドレスを含む。

【0016】本発明（請求項7）は、電子的な情報の流通を行う電子情報流通システムにおいて、トークンを特定するトークン情報を管理するトークン管理装置に搭載される電子情報流通プログラムを格納した記憶媒体であって、利用者装置で生成された保護データを特定する保護データIDとトークン情報を含む第1の情報を受信させる第1の通信プロセスと、保護データIDと等しい値を持つ第1の情報が既に蓄積されているかを判定する判定プロセスと、判定プロセスにおいて蓄積されていない時のみ第1の情報を蓄積手段に格納する格納プロセスと、既に蓄積手段に格納されている第1の情報に対する更新情報として該第1の情報を特定する保護データIDと更新後の新しいトークン情報を含む第2の情報を受信する第2の通信プロセスと、第2の情報の送信元の装置が第1の情報に含まれるトークン情報によって特定されるトークンを保有していることを検証する検証プロセスと、検証プロセスにおいて保有している時のみ第1の情報を更新する更新プロセスとを有する。

【0017】本発明（請求項8）は、検証プロセスにおいて、第2の情報の送信元からトークンを受信し、該トークンに対する一方向性関数の出力値が、更新対象の第1の情報に記録されているトークン情報に一致するかを検証する手段を含む。

1の情報に記録されているトークン情報に一致するかを検証するプロセスを含む。本発明（請求項9）は、蓄積手段に蓄積されている第1の情報に対する更新を行うために受信する第2の情報には、さらに、該第1の情報に含まれるトークン情報によって特定されるトークンを含み、該第2の情報の送信元の装置が、トークンを保有していることを判別するプロセスを含む。

【0018】本発明（請求項10）は、保護データIDを受信する第3の通信プロセスと、蓄積手段に格納されている第1の情報の中から保護データIDが含まれる第1の情報を検索し、該第1の情報に含まれるトークン情報を送信するプロセスとを更に有する。本発明（請求項11）は、電子的な情報の流通を行うための電子情報流通方法において、多重使用を防止すべき保護データを発行する際に、発行者装置において、保護データを生成し、利用者装置に転送し、利用者装置が保護データを受け取ると、該保護データ毎にトークンを生成して格納しておき、該トークンと該保護データからハッシュ値で表現される保護データIDとトークン情報を含む発行要求を生成して、該発行者装置に転送し、発行者装置は、発行要求に含まれているトークン情報を保護データIDを含むトークン情報登録要求を生成し、トークン管理装置に転送し、トークン管理装置は、トークン情報登録要求に含まれている保護データIDが蓄積されているかを判定し、蓄積されていない場合に、該保護データIDに対応するトークン情報を登録する。

【0019】本発明（請求項12）は、保護データを譲渡する際に、譲渡元の利用者装置において、譲渡対象の保護データを指定し、譲渡先の利用者装置に該保護データを転送し、譲渡先の利用者装置は、保護データに対応する新たなトークンを生成して格納しておき、保護データと新たなトークンのハッシュ値で表現されるトークン情報を含む譲渡要求を生成して、譲渡元の利用者装置に該譲渡要求を転送し、譲渡元の利用者装置は、蓄積されている譲渡対象の保護データに対するトークンを取得し、譲渡要求に含まれている該保護データに対する新しいトークン情報と保護データIDとトークンとを含むトークン情報更新要求を生成し、トークン管理装置に該トークン情報更新要求を転送し、トークン管理装置は、トークン情報更新要求に含まれているトークン情報を、予め蓄積されているトークン情報と一致するかを判定し、等しい場合に、保護データのトークン情報を更新する。

【0020】本発明（請求項13）は、保護データを消費する際に、利用者装置は、保護データ要求条件を受け取ると、その条件に合致する保護データを予め保護データが格納されている記憶手段から検索し、検索された保護データに対するトークンを取得し、改札者装置に該トークンと該保護データとを転送し、改札者装置は、保護データのハッシュ値で表現される保護データIDとトークンを含むトークン情報削除要求を生成し、トークン管

理装置に該削除要求を転送し、トークン管理装置は、トークン情報削除要求に含まれているトークンのハッシュ値と予め蓄積されているトークン情報と一致するかを判定し、等しい場合に、保護データのトークン情報を無効にする。

【0021】上記により、信頼できる第三者機関(ＴＴＰ)等が、保護データの生成者に代わって保護データの内容と、その所有者を管理することで、サービス提供者毎にセンタDBを運営する必要がなくなり、また、サービス提供者が勝手にセンタDB上にある保護データを削除あるいは、改ざんすることを防止することが可能となる。

【0022】

【発明の実施の形態】電子現金や電子チケットのような保護データは、一般に、発行、譲渡、使用(又は、改札)の3種類のトランザクションによって、発行者、利用者、サービス提供者の間を流通するものと見做すことができる。つまり、保護データは、発行者による発行トランザクションの実行によって生成されて利用者に渡り、利用者による譲渡トランザクションの実行により、利用者間を転々と流通し、最後に、サービス提供機関による改札トランザクション(あるいは、利用者による消費トランザクション)の実行により消滅する。

【0023】これを実現するために、本発明では、発行者、利用者、改札者がそれぞれ保有する発行者装置、利用者装置、改札者装置と、保護データが不正にコピーされることを防止するため、保護データが本物が複製かを識別する機構であるトークン管理装置と、これらの装置を接続するネットワーク装置(インターネット等)から構成される。

【0024】図2は、本発明の電子情報流通システムの構成を示す。同図に示す電子情報流通システムは、1つのネットワーク装置19に接続された1個以上のトークン管理装置11、12、1個以上の発行装置13、14、1個以上の利用者装置15、16、1個以上の改札者装置17、18から構成される。

【0025】発行装置13、14は、流通対象の電子情報(保護データ)を生成して転送する。利用者装置15、16は、発行装置で生成された保護データを受信し、当該電子情報の所有者を特定するトークン情報を生成して、蓄積する。トークン管理装置11は、保護データを特定する保護データIDとトークン情報を含む管理情報(保護データID+トークン情報)を受信し、保護データIDと等しい値を持つ別の情報が既に蓄積されているかを判定し、蓄積されていない時のみ、管理情報(保護データID+トークン情報)を蓄積する。また、既に管理情報が蓄積されている更新情報として管理情報を特定する保護データIDと更新後の新しい所有者を特定するトークン情報を含む更新情報(保護データID+新トークン情報)を受信し、当該更新情報の送信元の

装置が、管理情報(保護データID+トークン情報)に含まれるトークン情報によって特定されるトークンを保有していることを検証する。検証によりトークンを保有している時のみ、管理情報(保護データID+トークン情報)を更新情報に更新する。

【0026】ネットワーク装置19は、上記の各装置を接続する。

【0027】

【実施例】以下、図面と共に本発明の実施例を説明する。

【第1の実施例】図3は、本発明の第1の実施例のトークン管理装置の構成を示す。同図に示すトークン管理装置20は、トークン情報蓄積部21、記録制御部22、公開制御部23、及び通信部24から構成される。各部の詳細な動作は後述する。

【0028】図4は、本発明の第1の実施例の発行者装置の構成を示す。同図に示す発行者装置30は、通信部31、保護データ生成部32、発行制御部33から構成される。各部の詳細な動作は後述する。図5は、本発明の第1の実施例の利用者装置の構成を示す。同図に示す利用者装置40は、通信部41、譲渡制御部42、譲受制御部43、被改札制御部44、保護情報蓄積部45、及びトークン蓄積部46から構成される。各部の詳細な動作は後述する。

【0029】図6は、本発明の第1の実施例の改札者装置の構成を示す。同図に示す改札者装置50は、通信部51、改札制御部52から構成される。各部の詳細な動作は後述する。上記の各装置を用いて保護データの流通を安全に行う方式を、以下(1)保護データの発行を行う発行トランザクションの場合、(2)保護データの譲渡を行う譲渡トランザクションの場合、(3)保護データの消費(改札)を行う消費(改札)トランザクションの場合に分けて説明する。なお、各装置を跨ぐるそれぞれの通信は、ネットワーク装置19を介するものとする。

【0030】(1)発行トランザクション:図7は、本発明の第1の実施例の保護データの発行を行う場合のシーケンスチャートである。

ステップ601) 発行者装置30の発行制御部33は、保護データ生成部32により、保護データMを生成する。保護データMは、例えば、電子チケットの場合には、電子チケットが表象する権利の内容が記述されたデジタル情報である。但し、トークン管理装置20が複数存在することを前提とするシステムでは、この保護データMの中に、トークン管理装置20の識別子が含まれているものとする。また、保護データMの内容に対して否認防止や改ざん防止が求められる場合には、発行者による署名が施される場合もあるが、保護データMにはこれらの署名も含まれるものとする。

【0031】ステップ602) 発行者装置30の発行

制御部33は、通信部31により、利用者装置40に保護データMを転送する。

【0032】ステップ603) 利用者装置40の譲受制御部43は、通信部41により保護データMを受け取ると、乱数K₀を生成する。このように、乱数K₀は、保護データM毎に1つ生成されるものであり、これを保護データMのトークンと呼ぶ。

【0032】ステップ604) 譲受制御部43は、保護データ蓄積部45に保護データMを、トークン蓄積部46にK₀を格納する。ここで、保護データは、必ずしも秘密にしておく必要がないため、保護データ蓄積部45の内容は、利用者が管理するサーバ等で公開してもよい。一方、トークンK₀は、利用者装置40の内部に安全に保管され、漏れないことを前提とする。

【0033】ステップ605) 譲受制御部43は、これらトークンK₀と保護データMから発行要求

$$R_0 = (h(M), h(K_0))$$

を生成する。ここで、h(X)は、Xのハッシュ値であり、この関数を実現する方法としては、RSA Data Security社のMD5や、米国NISTによって規定されたSHA等がある。

【0034】ステップ606) 譲受制御部43は、通信部41により、生成した発行要求R₀を発行者装置30に送る。

【0035】ステップ607) 発行者装置30の発行制御部33は、通信部31により受け取った発行要求R₀から保護データMに対するトークンの登録要求

$$IO_0 = (h(M), nil, h(K_0))$$

を生成し、通信部31によりトークン管理装置20に登録要求IO₀を転送する。ここで、h(M)を保護データID、h(K₀)をトークン情報と呼ぶ。

【0036】ステップ608) トークン管理装置20の記録制御部22は、通信部24より受け取ったトークン登録要求IO₀に含まれている保護データID h(M)とトークン情報h(K₀)をトークン情報蓄積部21に格納する。具体的には、

① トークン情報蓄積部21は、図8に示す構造のトークン情報管理テーブル90を保持する。このとき、既に登録されている場合、即ち、保護データID h(M)がh(m₁)…h(m_n)の何れかに一致するかどうかチェックする。

② ①の結果、もし一致するものが存在した場合には、例外を発生させ、発行トランザクションを例外終了させる。

③ ①の結果、いずれにも一致しなかった場合には、保護データIDが保護データID h(M)、トークン情報履歴が<nil, h(K₀)>という内容の行を追加する。これにより、保護データMのトークン情報は、h(K₀)と解釈することとする。つまり、K₀が保護データMのトークンとして解釈されることになる。但し、

後で述べるように、トークン情報は、譲渡トランザクションによって更新される可能性がある。

【0036】ステップ609) トークン管理装置20の記録制御部22は、ステップ608が成功すると、通信部24によりSUCCESSイベントを発行者装置30に転送する。以上、ステップ601～609のステップの処理により、発行の基本的なフローは終了する。

【0037】以下に示すステップ610～614は、保護データを受け取った利用者装置40が、それが本当に自分のものであるかを検証するステップであり、省略可能である。また、これは、発行トランザクションの一部として行うこともできるし、利用者が指定した別のタイミングで行うこともできる。

【0038】ステップ610) 利用者装置40の譲受制御部43は、利用者からの指示やタイマからのイベント等を受信したことを契機に、保護データMに対するトークン情報がトークン管理装置に登録されているかを検証する要求を生成する。

【0039】ステップ611) 利用者装置40は、通信部41により保護データMに対するトークン情報の検索要求としてh(M)を転送する。

【0040】ステップ612) トークン管理装置20の公開制御部23は、通信部42よりトークン情報の検索要求として、h(M)を受け取ると、トークン情報蓄積部21に格納されているトークン情報管理テーブル90から、保護データIDとしてh(M)を有する最新のトークン情報を検索する。

【0041】ステップ613) 公開制御部23は、ステップ612によって検索された最新のトークン情報を通信部24によって利用者装置4に転送する。なお、ステップ611～ステップ613で行っている処理は、h(M)をキーとして、トークン情報を検索して返す単純な処理であるため、IETFで標準化されているHTTPプロトコルを用いて実現してもよい。

【0042】ステップ614) 利用者装置40の譲受制御部43は、通信部41より最新のトークン情報を受け取ると、それがトークン蓄積部46に格納されているK₀のハッシュ値と一致するかを検証する。もし、一致すれば、自分が所有であることが確認できる。なぜなら、以上のシーケンスチャートから明らかのように、トークンK₀は、利用者装置40自身で生成し、かつ外には出ないため、トークンK₀を知っているのは、利用者装置40の保有者のみであるからである。

【0043】(2) 譲渡トランザクション：以下の例では、トークン管理装置20を介して、2つの利用者装置40aと40b間で保護データの譲渡を行う場合について説明する。図9は、本発明の第1の実施例の保護データ譲渡の場合の動作を示すシーケンスチャートである。

【0044】ステップ701) 利用者装置40aの制

御部42は、利用者に保護データ蓄積部45に格納されている保護データの一覧を表示すること等により、譲渡対象の保護データMを指定する。

ステップ702) 利用者装置40aの譲渡制御部42は、通信部41により、譲渡先の利用者装置40bに保護データMを転送する。

【0043】ステップ703) 利用者装置40bの譲受制御部43は、通信部41により保護データMを受け取ると、乱数K_jを生成する。この乱数K_jは、譲渡トランザクションが成功した後、保護データMの新しいトークンとなる。

ステップ704) 利用者装置40bの譲受制御部43は、保護データ蓄積部45に保護データMを、トークン蓄積部46にトークンK_jを格納する。

【0044】ステップ705) 利用者装置40bの譲受制御部43は、トークンK_jと保護データMから譲渡要求

$$R_j = (h(M), h(K_j))$$

を生成する。ステップ706) 利用者装置40bの譲受制御部43は、通信部41により、生成した譲渡要求R_jを利用者装置40aに送る。

【0045】ステップ707) 利用者装置40aの譲渡制御部42は、トークン蓄積部46から譲渡対象の保護データMに対するトークンK_{j-1}を取得する。

ステップ708) 利用者装置40aの譲渡制御部42は、通信部41により受け取ったR_jとステップ707で獲得したトークンK_{j-1}から保護データMに対するトークンの更新要求

$$I_O_j = (h(M), K_{j-1}, h(K_j))$$

を生成し、通信部41によりトークン管理装置20に更新要求I_{Oj}を転送する。

【0046】ステップ709) トークン管理装置20の記録制御部22は、通信部24より受け取った更新要求I_{Oj}に含まれているh(K_j)を保護データMに対する新しいトークン情報としてトークン情報蓄積部21に格納する。具体的には、

① トークン情報蓄積部21が保持するトークン情報管理テーブル90(図8)において、h(M)=h(m_i)なるh(m_i)が存在するかどうか調べる。

② ①の結果、存在しない場合には、例外を発生させ、譲渡トランザクションを例外終了する。

③ ①の結果、存在する場合には、末尾のトークン更新履歴<k_{i,j-2}, h(k_{i,j-1})>(j>1, j=1のとき、k_{i,j-2}=n_{i1})中のh(k_{i,j-1})と、受け取った更新要求I_{Oj}のトークンK_{j-1}から計算したh(K_{j-1})の値が等しいかチェックする。

④ ③の結果、等しくない場合には、例外を発生させ、譲渡トランザクションを例外終了させる。

⑤ ③の結果、等しい場合には、新たな更新履歴として、<k_{j-1}, h(K_j)>を追加する。これにより、

保護データMのトークン情報はh(K_j)に更新されたと解釈する。つまり、K_jがMの唯一のトークンとして解釈されることになる。

【0047】ステップ710) トークン管理装置20の記録制御部22は、ステップ709が成功すると、通信部24によりSUCCESSイベントを利用者装置40aに転送する。以上、ステップ701~710のステップの処理により、譲渡の基本的なフローは終了する。

【0048】以下に示すステップ711~715は、保護データを受け取った利用者装置40bが、それが本当に自分のものであるかを検証するステップであり、省略可能である。また、これは、譲渡トランザクションの一部として行うこともできるし、利用者が指定した別のタイミングで行うこともできる。

ステップ711) 利用者装置40bの譲受制御部43は、利用者からの指示やタイマからのイベント等を受信したことを契機に、保護データMに対する新しいトークン情報がトークン管理装置20に登録されているかを検証する要求を生成する。

【0049】ステップ712) 利用者装置40bは、通信部41により保護データMに対するトークン情報の検索要求としてh(M)を転送する。

ステップ713) トークン管理装置20の公開制御部23は、通信部24より、トークン情報の検索要求としてh(M)を受け取ると、トークン情報蓄積部21に格納されているトークン情報管理テーブル90(図8)から保護データIDとしてh(M)を有する最新のトークン情報を検索する。

【0050】ステップ714) 公開制御部23は、ステップ712によって検索された最新のトークン情報を通信部24によって利用者装置40に転送する。なお、ステップ712~ステップ714で行っている処理は、h(M)をキーとしてトークン情報を検索して返す単純な処理であるため、IEFTで標準化されているHTTPプロトコルを用いて実現してもよい。

【0051】ステップ715) 利用者装置40bの譲受制御部43は、通信部41より最新のトークン情報を受け取ると、当該トークン情報がトークン蓄積部46に格納されているK_jのハッシュ値と一致するかを検証する。もし、一致すれば、自分が所有者であることが確認できる。なぜなら、以上のシーケンスチャートから明らかなように、K_jは、利用者装置40b自身で生成し、かつ外には出ないため、K_jを知っているのは、利用者装置40bの保有者のみであるからである。

【0052】ある保護データM(=m_i)が、以上で述べたシーケンスチャートにより、発行者装置30により発行され、j個の利用者装置40間で譲渡が行われたとすると、図8に示すような

$$<n_{i1}, h(k_{i,0})>, <k_{i,0}, h(k_{i,1})>, \dots, <k_{i,j-1}, h(k_{i,j})>$$

というトークン情報更新履歴が作られる。この結果、流通過程で生成されたトークン $k_{i,0}, \dots, k_{i,j-1}$ は、公開され、無効なものとなり、唯一 $k_{i,j}$ のみが公開されない。このため、 $k_{i,j}$ を知っている最後に譲渡された者のみが有効な所有者とすることができます。

【0053】(3) 消費(改札)トランザクション: 図10は、本発明の第1の実施例の保護データ更新の場合の動作を示すシーケンスチャートである。

ステップ801) 改札者装置50の改札制御部52は、通信部51により、改札対象の利用者装置40に保護データ要求条件を転送する。保護データ要求条件の指定方法の詳細は述べないが、改札対象の保護データに含まれる属性値などに関する条件を指定する。

【0054】ステップ802) 利用者装置40の被改札制御部44は、通信部41により、保護データ要求条件を受け取ると、その条件に合致する保護データMを保護データ蓄積部45から検索し、取得する。

ステップ803) ステップ802によって取得した保護データMに対するトークン K_j を取得する。

【0055】ステップ804) 利用者装置40の被改札制御部44は、通信部41により、改札者装置50に保護データM及びトークン K_j を転送する。

ステップ805) 改札者装置50の改札制御部52は、通信部51により受け取った保護データM及びトークン K_j から保護データMに対するトークンの削除要求 $IO_{j+1} = (h(M), K_j, n_{i1})$ を生成し、通信部51によりトークン管理装置20に当該削除要求 IO_{j+1} を転送する。

【0056】ステップ806) トークン管理装置20の記録制御部22は、通信部24より受け取った削除要求 IO_{j+1} の $h(M)$ によって指定されるトークン情報を無効にする。具体的には、

① トークン情報蓄積部21が保持するトークン情報管理テーブル90(図8)において、 $h(M) = h(m_i)$ なる $h(m_i)$ が存在するかどうか調べる。

② ①の結果、存在しない場合には、例外を発生し、改札トランザクションを例外終了する。

③ ①の結果、存在する場合には、末尾のトークン更新履歴 $< k_{i,j-1}, h(k_{i,j}) >$ 中の $h(k_{i,j})$ と、受け取った IO_{j+1} 中の K_j から計算した $h(K_j)$ の値が等しいかチェックする。

④ ③の結果、等しくない場合には、例外を発生させ、譲渡トランザクションを例外終了させる。

⑤ ③の結果、等しい場合には、新たな更新履歴として、 $< K_j, n_{i1} >$ を追加する。これにより、保護データMのトークン情報は、 n_{i1} に更新されたと解釈する。つまり、保護データMのトークンは存在しないものと解釈されることになる。

【0057】ステップ807) トークン管理装置20の記録制御部22は、ステップ806が成功すると、通

信部24により、SUCCESSイベントを改札者装置50に転送する。

ステップ808) 改札者装置50の改札制御部52は、利用者装置40あるいは、利用者に対して、保護データMを改札した引換えとして、サービスや物を提供する(保護データがチケットの場合)。

【0058】上記で示したシーケンスチャートによる実施例は本発明における一例であり、本発明の別の実施例として以下に示すような例も可能である。

【第2の実施例】前述の第1の実施例の図7に示す発行トランザクションにおけるステップ606とステップ607をマージして、利用者装置40からトークン管理装置20に対して直接トークンの登録要求 IO_0 を送付してもよい。

【0059】同様に、図9における譲渡トランザクションにおけるステップ707をステップ702の前に行い、ステップ702において、予め利用者装置40aから利用者装置40bに保護データMと一緒にトークン K_0 を転送しておくことにより、ステップ706とステップ708をマージして利用者装置40bから利用者装置40aに対して、直接トークンの登録要求 IO_j を送付してもよい。

【0060】同様に、図10における消費(行使)トランザクションにおけるステップ804とステップ805をマージして、利用者装置40から改札者装置50に対して直接 IO_{j+1} を送付してもよい。

【第3の実施例】トークン管理装置20におけるトークン情報蓄積部21に記録されるトークン情報の管理テーブル90の構造は一例であり、例えば、図11に示すように、トークン情報の変更履歴を全て保管するのではなく、各保護データ m_i に対するその時点での有効なトークン情報 $h(k_{i,j})$ のみを保管するようにしてもよい。

【0061】この場合でも、上記の実施例と同様に、このトークン情報を更新あるいは無効ができるのは、 $k_{i,j}$ を持っている利用者装置40だけである。

【第4の実施例】トークン管理装置20に、課金機能を付与し、トークン情報登録要求、あるいは、トークン情報更新要求、あるいは、トークン情報無効化要求毎に、利用料を徴収することも可能である。

【0062】課金機能の実現方法については、詳細は述べないが、例えば、トークン管理装置20の利用を会員制とし、トークン管理装置20の利用に先立ち特定の会員証(デジタル証明書)等による認証を行い、利用履歴を記録し、クレジットカードや銀行振込により、利用者頻度に応じて使用料を徴収する方法、compaq社のMicracentやRivestらのPayword等のマイクロペイメント方法等様々な方法が考えられる。

【0063】また、トークン情報には、有効期限を付与し、有効期限内でのみ、トークン情報の公開を行うこともできる。有効期限の付与は、トークン管理装置20毎

に与える方法、保護データ単位に与える方法、トークン情報単位に与える方法等がある。特に、トークン情報を単に与えた場合には、利用者装置40は、自分自身の利用者装置40に譲渡することで、トークンを更新することにより、有効期限を延長することもできる。この機能と課金処理を組み合わせることにより、利用時間に応じて料金を徴収するシステムをトークン管理装置によって代行することも可能となる。

【0064】また、上記の実施例では、図7～図10のシーケンスチャートに基づいて説明しているが、この例に限定されることなく、各シーケンスチャートにおける装置毎にその動作をプログラムとして構築し、本発明を実施する際に、発行者装置30、利用者装置40、トークン管理装置20及び改札装置50として利用されるコンピュータに接続されるディスク装置や、フロッピー

(登録商標)ディスク、CD-ROM等の可搬記憶媒体に格納しておき、本発明を実施する際にインストールすることにより、容易に本発明を実現することが可能である。

【0065】なお、本発明は、上記の実施例に限定されることなく、特許請求の範囲内において種々変更・応用が可能である。

【0066】

【発明の効果】上述のように、本発明によれば、保護データの内容に依存せずに、保護データ毎に存在するトークンをただ一つに限定することができるので、トークンを保持しているかどうかで保護データの正当な所有者かどうかを識別することができる。これにより、保護データが不正に複数の利用者に転送されても、更には、たとえ、公開情報となつても、保護データの正規の所有者かどうかを判定することができる。しかも、保護データに対する正当なトークンを所有している者は、自分がその保護データの唯一の所有者であることを、誰にも(トークン管理装置にさえ)知られることなく、確認することができる。

【0067】また、トークン自体の管理は、利用者あるいは、利用者装置に任せているので、ICカード等の耐タンパ装置だけではなく、利用者の責任でハードディスク等に自由に複製をとることも可能である。それでも、保護データが譲渡あるいは、消費された場合には、その利用者が保持しているすべてのトークンは無効化されるので、二重譲渡や、二重使用は防止することができる。

【0068】また、トークン管理装置を利用するにあたっては、本発明の利用者装置を保持するだけでよく、特定の機関から発行されたディジタル証明書等を事前に取得しておく必要はない。また、保護データの所有者かどうかは使い捨ての乱数で生成したトークンが使われるので、匿名性を保証できる。

【0069】さらに、アルゴリズムとしては、計算量を

必要とする公開鍵方式を必須とせず、ハッシュ関数のみで実現できるため、極めて高速に処理を行うことができる。

【図面の簡単な説明】

【図1】本発明の原理構成図である。

【図2】本発明の電子情報流通システムの構成図である。

【図3】本発明の第1の実施例のトークン管理装置の構成図である。

【図4】本発明の第1の実施例の発行者装置の構成図である。

【図5】本発明の第1の実施例の利用者装置の構成図である。

【図6】本発明の第1の実施例の改札者装置の構成図である。

【図7】本発明の第1の実施例の保護データ発行の場合の動作を示すシーケンスチャートである。

【図8】本発明の第1の実施例のトークン情報の管理テーブルである。

【図9】本発明の第1の実施例の保護データ譲渡の場合の動作を示すシーケンスチャートである。

【図10】本発明の第1の実施例の保護データ行使の場合の動作を示すシーケンスチャートである。

【図11】本発明の第3の実施例のトークン情報の管理テーブルの例である。

【符号の説明】

1 1, 1 2, 2 0, 2 0 0 トークン管理装置

1 3, 1 4, 3 0, 3 0 0 発行者装置

1 5, 1 6, 4 0, 4 0 0 利用者装置

1 7, 1 8, 5 0 改札者装置

1 9, 1 0 0 ネットワーク装置

2 1 トークン情報蓄積部

2 2 記録制御部

2 3 公開制御部

2 4 通信部

3 1 通信部

3 2 保護データ生成部

3 3 発行制御部

4 1 通信部

4 2 譲渡制御部

4 3 譲受制御部

4 4 被改札制御部

4 5 保護データ蓄積部

4 6 トークン蓄積部

5 1 通信部

5 2 改札制御部

1 0 0 ネットワーク装置

2 0 0 トークン管理装置

2 0 1 第4の通信手段

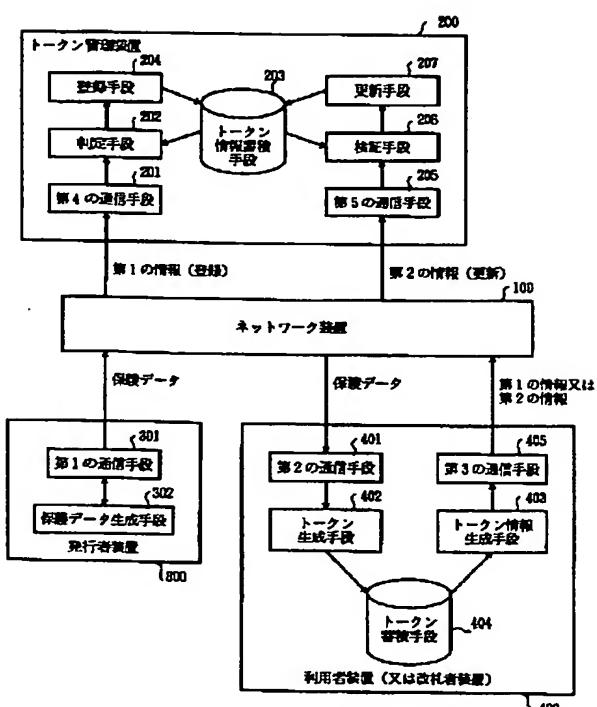
2 0 2 判定手段

203 トーケン情報蓄積手段
 204 登録手段
 205 第5の通信手段
 206 検証手段
 207 更新手段
 208 発行者装置
 301 第1の通信手段

302 保護データ生成手段
 400 利用者装置（または、改札者装置）
 401 第2の通信手段
 402 トーケン生成手段
 403 トーケン情報生成手段
 404 トーケン蓄積手段
 405 第3の通信手段

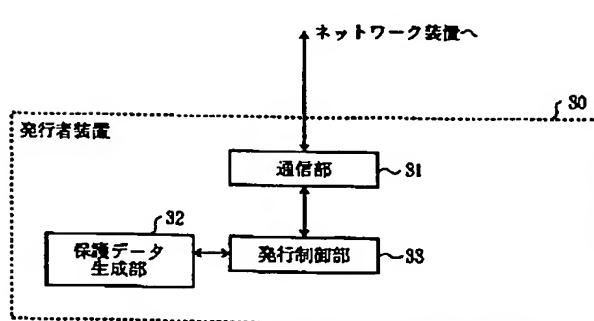
【図1】

本発明の原理構成図



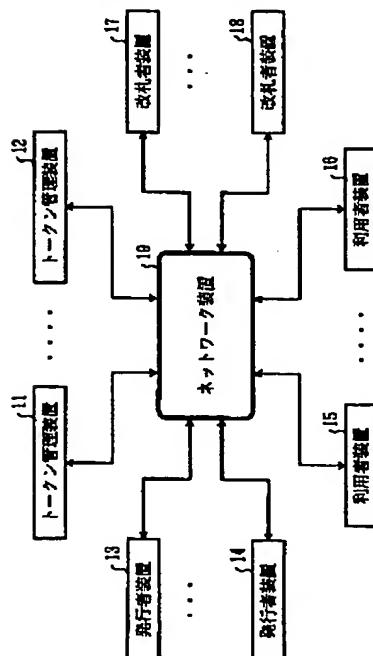
【図4】

本発明の第1の実施例の発行者装置の構成図



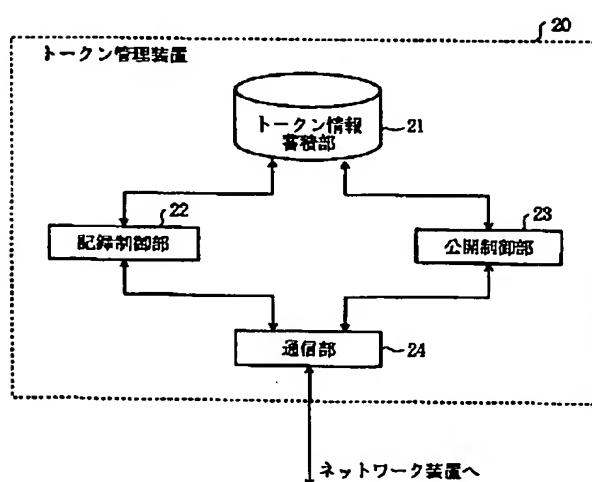
【図2】

本発明の電子情報流通システムの構成図



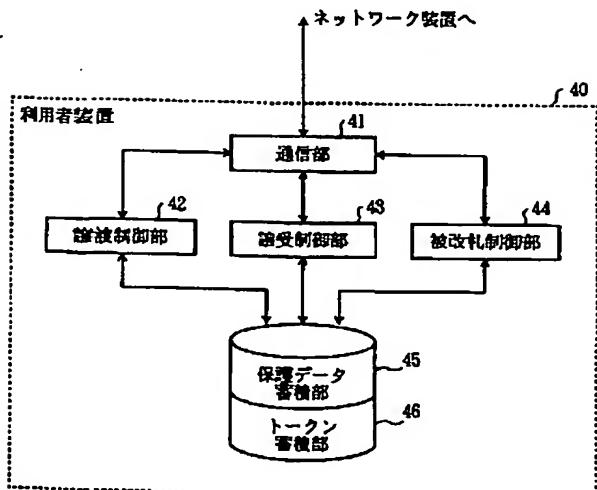
【図3】

本発明の第1実施例のトーケン管理装置の構成図



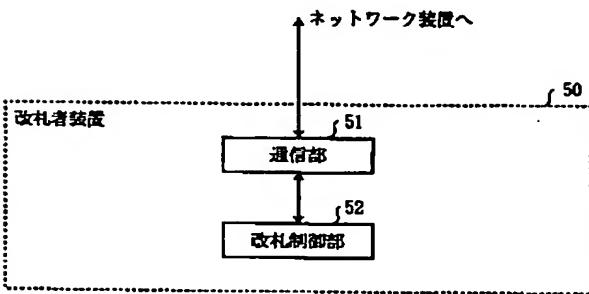
【図5】

本発明の第1の実施例の利用者装置の構成図



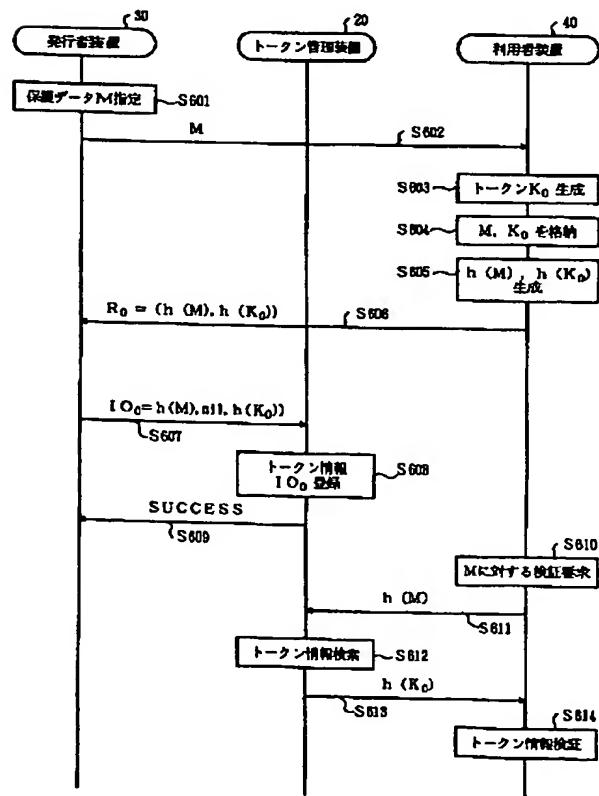
【図6】

本発明の第1の実施例の改札者装置の構成図



【図7】

本発明の第1の実施例の保護データ発行の場合の動作を示すシーケンスチャート

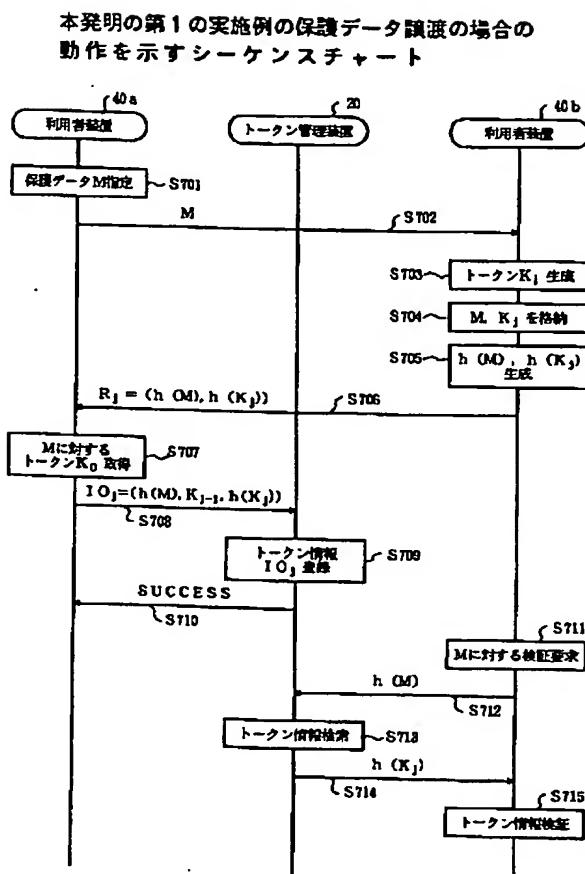


【図8】

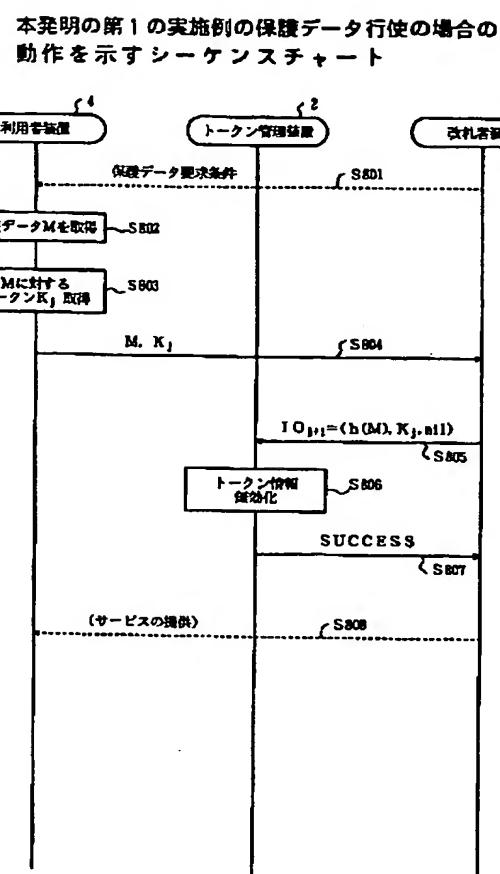
本発明の第1の実施例のトークン情報の管理テーブル

| 保護データID | トークン情報更新履歴 | |
|---------|--|--|
| | h(m1) | h(m2) |
| | <nil, h(k1,0), h(k1,1)>, ... <k1,p-1, h(k1,p)> | <nil, h(k1,0), h(k1,1)>, ... <k1,p-1, h(k1,p)> |
| | ⋮ | ⋮ |
| | <nil, h(kn,0), h(kn,1)>, ... <kn,p-1, h(kn,p)> | <nil, h(kn,0), h(kn,1)>, ... <kn,p-1, h(kn,p)> |
| | ⋮ | ⋮ |
| | h(mn) | h(mn) |

【図 9】



【図 10】



【図 11】

本発明の第3の実施例のトーカン情報の管理テーブル
(別の実施例)

100

| 保護データID | トーカン情報 | |
|----------|--------------|------|
| $h(m_1)$ | $h(k_{1,j})$ | ~101 |
| ... | ... | |
| $h(m_i)$ | $h(k_{i,j})$ | ~102 |
| ... | ... | |
| $h(m_n)$ | $h(k_{n,x})$ | ~103 |

フロントページの続き

(51) Int. Cl. 7

識別記号

F I

テーマコード(参考)

G 0 6 F 15/30

3 6 0

15/40

3 1 0 F

3 1 0 C

3 7 0 Z

15/411

310

(72)発明者 寺田 雅之
東京都千代田区大手町二丁目3番1号 日
本電信電話株式会社内

F ターム(参考) 5B049 AA05 BB11 BB46 BB61 CC05
CC16 CC39 DD04 DD05 EE03
EE05 EE23 FF09 GG04 GG07
GG10
5B055 BB10 CB09 CB10 EE02 EE03
EE17 EE21 EE27 FA05 FB03
HA12 JJ05 KK01 KK09
5B075 KK03 KK07 KK13 KK33 ND03
ND20 ND23 NK10 NK13 NK24
NK45 NK54 PP30 PQ05 PR03
UU40
5J104 AA07 KA01 NA12 PA07 PA12